SCIENTIFIC REPORTS
natureresearch

OPEN

Traceable Quantum Steganography Scheme Based on Pixel Value Differencing

Jia Luo[1,2], Ri-Gui Zhou[1,2*], GaoFeng Luo[1,2,3], YaoChong Li[1,2] & GuangZhong Liu[1*]

A novel and traceable quantum steganography scheme based on pixel value differencing (PVD) is proposed. In the proposed scheme, a quantum cover image is divided into non-overlapping blocks of two consecutive pixels. Then, by a series of reversible logic circuits, we calculate the difference value based on the values of the two pixels in each block and classify it as one of a set of continuous ranges. The secret image and operator information are embedded in the cover image by using the new obtained difference value to replace the original one. The number of bits of secret image that can be embedded in a block is determined, and the number of bits of operator information is decided by the range of the difference value belongs to. Moreover, when the embedded data is extracted from a stego image, it is not necessary to refer to the original cover image. The performance of the proposed scheme is based on the analysis of several categories of simulation results, such as visual quality, capacity, and robustness.

In recent decades, an increasing number of researchers have invested in the field of quantum image processing. Firstly, Vlasov[1] proposed a method of recognizing orthogonal images. Later, G. Beach *et al.*[2] showed that quantum algorithms like Grover algorithm[3] can be used for image processing tasks. And then, the investigations about capturing and storing digital image on a quantum computer were explored. There are already a series of quantum representation models, such as Qubit Lattice[4,5], Real Ket[6] and so on. Among them, flexible representation of quantum images (FRQI)[7] and a novel enhanced quantum representation of digital images (NEQR)[8] are widely adopted. Then, on the basis of FRQI and NEQR, researchers have contributed to quantum image processing algorithms and applications, such as quantum image translation[9,10], quantum image scaling[11–15], quantum image feature extraction[16], quantum image matching[17–19], and so on[20].

Especially quantum information hiding strategies have aroused considerable research interest, including quantum image steganography and quantum image watermarking. Like with classical steganography[21], which has been thoroughly studied, quantum image steganography aims to make secret data concealed in the cover image undetectable by external observers.

Since the least significant bit (LSB) method hides secret information to a cover image in a simple way, it gained more and more researchers' attention. In 2015, Jiang *et al.* proposed two quantum image steganography schemes based on moire patterns[22] and LSB[23], respectively. In 2016, Sang *et al.*[24] constructed a scheme in which quantum color image is the cover image. Using basic gates, Miyake *et al.*[25] designed quantum circuits to achieve the aim of embedding secret information. And Heidari *et al.*[26] investigated three methods to embed the secret data to red-green-blue channels. Furthermore, in 2017, Heidari *et al.*[27–30] also proposed some LSB based methods to protect copyright. Zhou *et al.*[31] proposed a scheme that includes three processes of extension, scrambling and embedding. A scheme based on embedding color watermark image is proposed by Li *et al.*[32]. Zhou *et al.*[33] proposed a watermarking scheme adopting new scrambling transformation in 2018.

To improve the performance of robustness of the existing quantum steganography algorithm, we proposed a quantum steganography scheme based on pixel value differencing (PVD). The concept of PVD was first proposed in ref.[34]. Because the human visual system has such a characteristic that human eyes are more sensitive to pixel modification of the smooth area of an image than the edge one, the amount of modification that each pixel of the digital image can tolerate is different. That is, without causing perceptible sensory distortion, each pixel can embed a different number of secret bits. But the amount of modification per pixel is uniform in the LSB

[1]College of Information Engineering, Shanghai Maritime University, Shanghai, 201306, China. [2]Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai, 201306, China. [3]College of Information Engineering, Shaoyang University, Shaoyang, 422000, China. *email: rgzhou@shmtu.edu.cn; gzhliu@shmtu.edu.cn

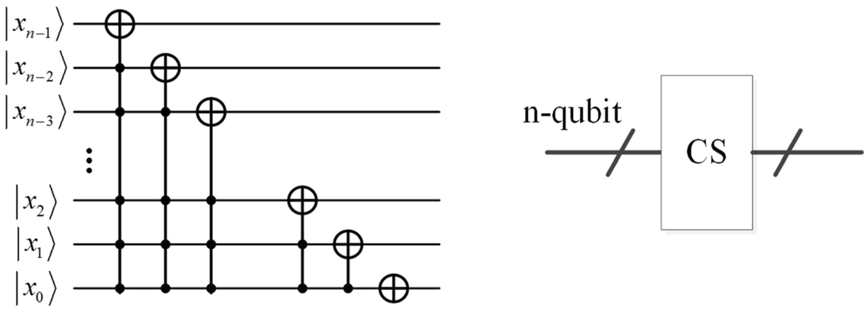


Figure 1. The cyclic shift transformation for one unit. It is consisting of a series of Controlled-NOT gates, and the number of control qubits is from n-1 to 0. The simplified module is shown on the right.

steganography algorithm. The LSB steganography algorithm does not consider the character and ignores the edge effect of the image, so the algorithm performance is general. Considering the image edge effect and human visual system characteristics, each pixel in the digital image can be tolerated different bits in the PVD algorithm.

The proposed steganography scheme divides the cover image into blocks of two pixels that do not overlap. If the pixel difference of the pixel block is small, it indicates that this block is in the smoothing region. That means the human eye is more sensitive to it, and only less secret data can be hidden. Conversely, if the pixel difference value of block is large, it indicates that the block is located in the edge region of the image. The human eye is less sensitive to it, and more secret information can be embedded. The secret information includes a secret image and operation information, wherein the operation information may include operator information, operation time, etc., that can be used to trace the secret image.

Preliminaries

The novel enhanced quantum representation for digital images (NEQR). NEQR model[8] uses the basis state of a qubit sequence to store the grayscale value of pixels in the image. Therefore, two entangled qubit sequences are used in NEQR to store the whole image. For a $2^n \times 2^n$ quantum image with ranged of 2^q, the representative expression of NEQR image is expressed as follows:

$$|I\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle \otimes |YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{k=0}^{q-1}|C_{YX}^k\rangle \otimes |YX\rangle \tag{1}$$

where q-qubit sequence $|C_{YX}^k\rangle = |C_{YX}^{q-1} \cdots C_{YX}^1 C_{YX}^0\rangle$ encodes the grayscale value $f(Y, X)$ of the corresponding pixel (Y, X) and $|YX\rangle = |y_{n-1} \cdots y_1 y_0\rangle |x_{n-1} \cdots x_1 x_0\rangle$ represents the position information in vertical and horizontal directions.

The pixel value differencing method (PVD). PVD method is first proposed in ref. [34], in which, a cover image is partitioned into non-overlapping blocks of two consecutive pixels, say p_i and p_{i+1}. A difference value d is calculated from the values of the two pixels by subtraction operation, which may be in the range from −255 to 255. Only consider the absolute values of d_i and classify them into a number of contiguous ranges, called R_i, where $i = 1, 2 \ldots n$. The number of bits can be embedded in a pixel pair is decided by which range the difference value belongs to. The difference value then is replaced by a new value to embed the bits of the secret information. This method provides an easy way to produce a more imperceptible result than those yielded by simple least significant bit (LSB) replacement methods. And also, the embedded secret information can be extracted from the stego image without referencing the original cover image.

Reversible logic circuits. In this section, a series of reversible logic circuits is predefined to accomplish the PVD method. More details are described as follows.

Cyclic shift transformation (CS). The cyclic shift is the realization of the position shifting transformation that was proposed in ref. [35]. The reversible logic circuit is illustrated in Fig. 1, and its function can be expressed as

$$|x_{n-1}\, x_{n-2} \ldots x_2\, x_1\, x_0\rangle \rightarrow |(x_{n-1}\, x_{n-2} \ldots x_2\, x_1\, x_0 + 1) \bmod 2^n\rangle \tag{2}$$

where n is the number of qubits in cyclic shift transformation.

Therefore, when we move the image to the left by one unit, the pixels will be transformed from $|f(Y, X)\rangle$ to $|f(Y, X+1)\rangle$.

Plain adder module (ADDER). The addition of two qubit sequences $|A\rangle$ and $|B\rangle$ by plain adder module is used in the proposed scheme that writes the result of the computation into one of the input sequences, i.e.

$$|A, B\rangle \rightarrow |A, A+B\rangle. \tag{3}$$

The reversible logic circuit of ADDER module[36] is shown in Fig. 2.

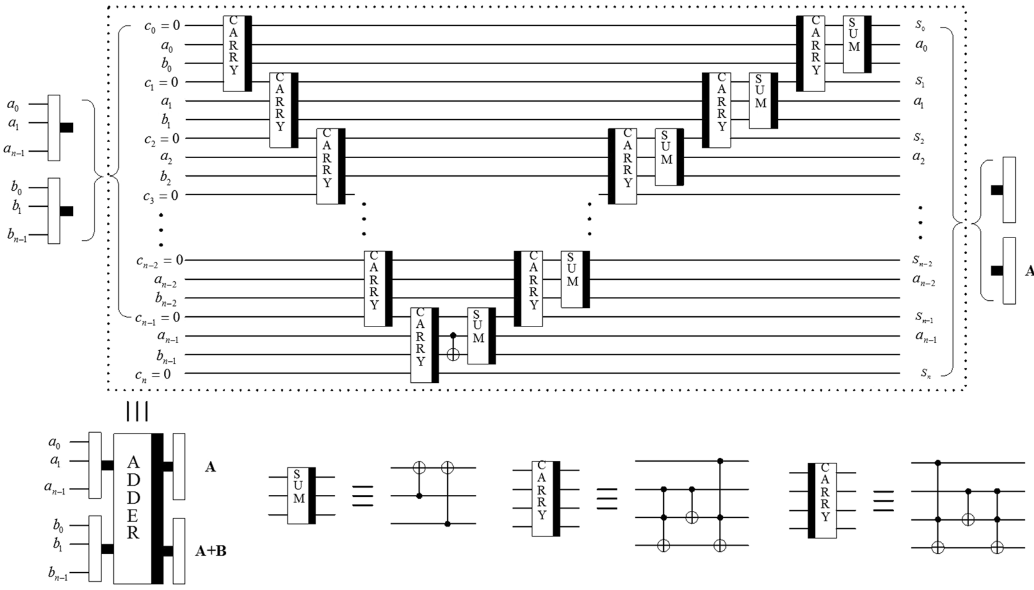


Figure 2. Circuit realization of plain adder module ADDER. The circuit in the dashed box implements the addition of two qubit sequences, and the three basic modules are illustrated below. The simplified module of ADDER is also given together.

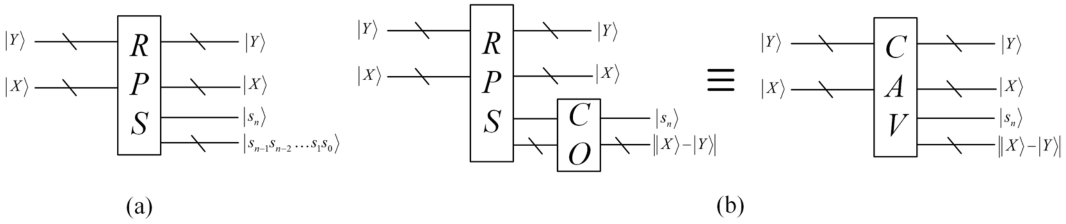

$|Y\rangle$
$|X\rangle$
RPS
$|s_n\rangle$
$|s_{n-1}s_{n-2}\dots s_1s_0\rangle$
CO
$\||X\rangle - |Y\rangle|$
CAV
(a)
(b)

Figure 3. (**a**) Simplified circuit module of RPS (**b**) Module of calculating the absolute value

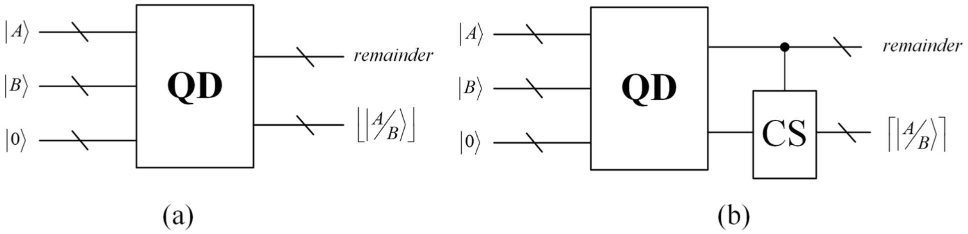


Figure 4. Quantum divider circuits (**a**) Round down quotient module (**b**) Round up quotient module. When the remainder is not equal to zero, the circuit module CS is adopted to round up the quotient.

Calculate the absolute value (CAV). Zhou *et al.*[15] designed a reversible parallel subtractor (RPS) through a series of basic modules. The simplified circuit module of RPS is illustrated in Fig. 3(a). There are two n-qubit inputs X and Y, where $|X\rangle = |x_{n-1}x_{n-2}\dots x_1x_0\rangle$ and $|Y\rangle = |y_{n-1}y_{n-2}\dots y_1y_0\rangle$. And the output $|S\rangle = |s_ns_{n-1}s_{n-2}\dots s_1s_0\rangle$ is the result of $|X - Y\rangle$. It is worth noting that the highest qubit s_n is the sign bit. When s_n is equal to 1, Y is greater than X and $|S\rangle$ is the complement code of difference value. When s_n is equal to 0, it means that X is greater than Y and $|S\rangle$ is difference value.

To calculate the absolute difference value, the reversible logic circuit implementing the complement operation (CO) is constructed. The integrated CAV module is shown in Fig. 3(b). For more details, please refer to ref.[15].

Quantum divider. The reversible logic circuit for implementation of division operation based on restoring division algorithm was proposed in[37]. Figure 4(a) illustrates a compendious quantum divider module. The inputs are $|A\rangle = |a_{n-1}a_{n-2}\dots a_1a_0\rangle$, $|B\rangle = |b_{n-1}b_{n-2}\dots b_1b_0\rangle$ and n ancillary qubits with an initial value of $|0\rangle$. The output contains the value of quotient that is rounded down. And we add a controlled cyclic shift operation mentioned in subsection 3.1 to the QD to acquire the round up quotient.

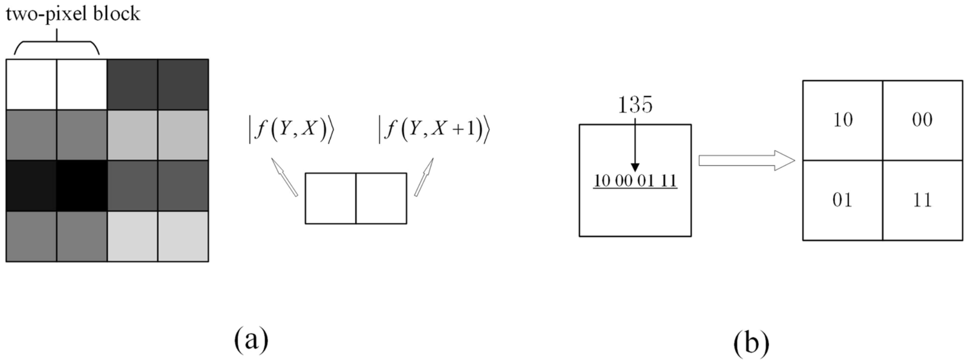


Figure 5. Two examples. (**a**) Example of the non-overlapping two-pixel blocks. The two pixels of same gray color in the image are the non-overlapping block. (**b**) Example of decomposing eight bits to four two-bits. The eight bits are divided into pairs, and then orderly filled into four positions.

Proposed Scheme

The secret image and the information of operator are embedded in cover image in the proposed traceable steganography scheme based on pixel value differencing. Wherein, the secret image is embedded regardless of the difference of the pixel values, and the operator information is embedded with different qubit numbers according to the level of the pixel value difference. Traceability of secret information is realizing by extracting operator information. More details are described next.

Quantization of differences of gray values of two-pixel blocks. Through analysis of the PVD method as described in subsection 2.2, it is known that the difference value d of $|f(Y,\ X)\rangle$ and $|f(Y,\ X+1)\rangle$ can be calculated by the reversible logic circuit CAV module so that we can partition the difference values in ranges R_i. Firstly, the way of dividing the square cover image into two-pixel blocks runs through all the rows of image in a consecutive and non-overlapping manner, and an example is shown in Fig. 5(a).

In general, small difference value indicates that the two-pixel block is in a smooth area, whereas a large difference value of a two-pixel block is corresponding to an edge area. The blocks in edge areas may, as mentioned previously, tolerate larger changes of pixel values than those in the smooth areas. Therefore, more information is embedded in edge areas than smooth areas.

Specifically, $|d\rangle$ is classified into a set of continuous ranges, say R_i where $i=0,\ 1\ldots 4$ as shown in Fig. 6. The proposed scheme is based on selecting the range widths of 8, 8, 16, 32, and 192, which partition the total range of [0,255] into [0, 7], [8, 15], [16, 31], [32, 63], [64, 255]. Two qubits in secret image are embedded in the pair pixels in every range. In contrast, the number of embedded operator information qubits varies with the difference value. That is, when the difference value is at R_0, it is not embedded. When it is at R_1, one qubit is embedded. By this analogy, when the difference value is at R_4, four qubits are embedded.

Data embedding. We propose a traceable steganography scheme utilizing the NEQR model, which hides a secret grayscale image and a bit stream (operator information) into a cover grayscale image. The size of secret image and cover image is $2^{n-1}\ \times\ 2^{n-2}$ and $2^n\ \times\ 2^n$, respectively. In order to correspond to the number of difference values, the secret image with $2^{n-1}\ \times\ 2^{n-2}$ and 8 bits grayscale is expanding to an image with $2^n\ \times\ 2^{n-1}$ and 2 bits grayscale. Figure 5(b) illustrates an example about how to decompose eight bits sequence into four two-bit sequences.

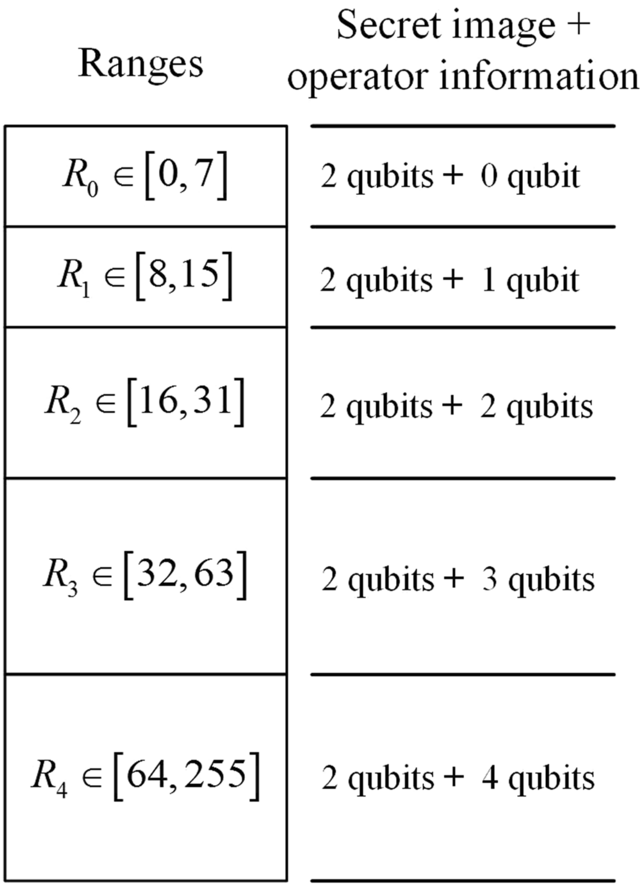
Then, the cover image and the decomposed secret image are transformed into quantum images $|C\rangle$ and $|S\rangle$, respectively. The representations can be expressed in Eq. (4):

$$\begin{aligned} |C\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,\ X)\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}|C_{YX}^{i}\rangle|YX\rangle \\ |S &= \frac{1}{2^{\frac{2n-1}{2}}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^{n-1}-1}|f(Y,\ X)|YX \\ &= \frac{1}{2^{(2n-1)/2}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^{n-1}-1}|S_{YX}^{1}S_{YX}^{0}\rangle|YX\rangle \end{aligned} \tag{4}$$

and the difference values of the cover image $|d\rangle$ are written as below:

$$|d\rangle = \frac{1}{2^{(2n-1)/2}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^{n-1}-1}\bigotimes_{i=0}^{7}|d_{YX}^{i}\rangle|YX\rangle. \tag{5}$$

To realize the partition of $|d\rangle$, based on thresholds the pixel value differences comparison operation U_t are proposed. The module of classification and the corresponding circuit is illustrated in the dotted box of Fig. 7. The number of t is changed according to the upper bound of ranges to be compared. Firstly, it is utilized to compare $|d\rangle$ with $|00000111\rangle$ that is the upper bound of first range and the parameter t is equal to 3 at this time. If the output



Ranges	Secret image + operator information
$R_0 \in [0,7]$	2 qubits + 0 qubit
$R_1 \in [8,15]$	2 qubits + 1 qubit
$R_2 \in [16,31]$	2 qubits + 2 qubits
$R_3 \in [32,63]$	2 qubits + 3 qubits
$R_4 \in [64,255]$	2 qubits + 4 qubits

Figure 6. Ranges of the difference value

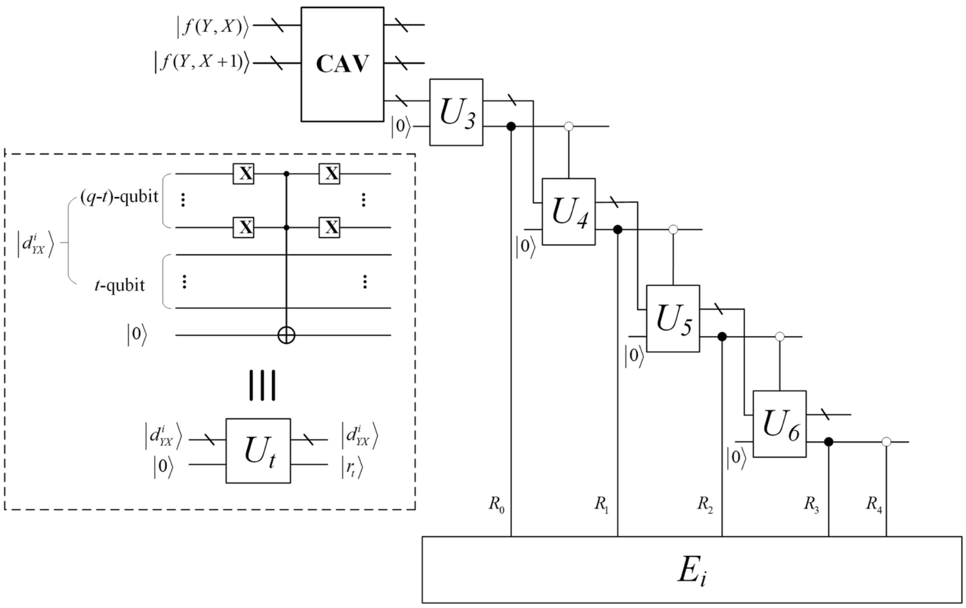


Figure 7. Circuits of classifying the difference value. In the dotted box, after flipping the highest q-t qubits using the X gates, a Controlled-NOT gate and an auxiliary qubit are used to assess if the highest q-t qubits are all zero, and then restore the original value with the same number of X gates. Four simplified module U_t are employed to divide the absolute difference value into five ranges, that is, R_0, R_1, R_2, R_3 and R_4. For different ranges, different E_i will be adopted. (The module E_i is described below)

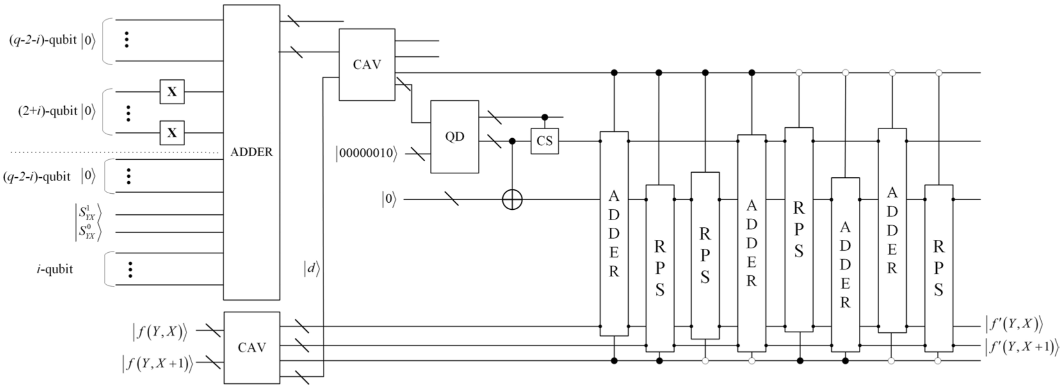


Figure 8. The embedding circuit E_i. i is the level of difference value range. Distinguishingly, when i = 0, the number of X gate is set to zero. The first ADDER module adds the lower bound of the range to the secret information qubits, and the result is subtracted from the pixel value difference. After dividing by 2 using the module QD, the round up or down quotient is added or subtracted from the original pixel values according to the constraint of Eq. (7).

$|r_i\rangle$ is equal to 1, it means that $|d\rangle$ is less than 8. That is, the range of $|d\rangle$ is R_1. If the output $|r_i\rangle$ is equal to 0, $|d\rangle$ is compared with the next upper bound. Similarly, all $|d\rangle$ can be partitioned in accordance with U_t, where $t = 3, 4, 5, 6$. For realizing the pixel value differencing and the determination of ranges, the whole reversible logic circuit is designed as shown in Fig. 7.

Since the number of embedded qubits in each range is confirmed, a new difference d' then is computed by:

$$d' = l_k + b_i \tag{6}$$

where b_i is the denary value of embedded qubits, that is consisted of 2-qubit in secret image and i-qubit in operator information. And the value b_i is in the range from 0 to $u_k - l_k$, hence the value of d' is in the range from l_k to u_k, where u_k and l_k represent the upper and lower bounds of the range R_k. According to the previous discussions, if we replace d with d', the resulting changes are presumably unnoticeable to the observer. Through a series inverse calculation, b_i is embedded in two-pixel block with pixel values of g_j and g_{j+1}, respectively. The function is defined to be:

$$|f(g_i, g_{i+1})\rangle = \begin{cases} |g_i + \lceil m/2 \rceil\rangle,\ |g_{i+1} - \lfloor m/2 \rfloor\rangle & \text{if } d_i' > d_i \text{ and } g_i \geq g_{i+1} \\ |g_i - \lfloor m/2 \rfloor\rangle,\ |g_{i+1} + \lceil m/2 \rceil\rangle & \text{if } d_i' > d_i \text{ and } g_i < g_{i+1} \\ |g_i - \lceil m/2 \rceil\rangle,\ |g_{i+1} + \lfloor m/2 \rfloor\rangle & \text{if } d_i' \leq d_i \text{ and } g_i \geq g_{i+1} \\ |g_i + \lceil m/2 \rceil\rangle,\ |g_{i+1} - \lfloor m/2 \rfloor\rangle & \text{if } d_i' \leq d_i \text{ and } g_i < g_{i+1} \end{cases} \tag{7}$$

where $|m\rangle = ||d' - d|\rangle$. The corresponding reversible logic circuit, that is module E_i, is demonstrated in Fig. 8. To assist one better comprehend the embedded procedure, an example of data embedding is illustrating in Fig. 9.

Extraction procedure.

The extraction procedure is as follows:

1. The stego image is divided into adjacent two-pixel blocks $\left(y_j', y_{j+1}'\right)$ according to the same partition method in the embedding step.
2. Calculate the difference value by Eq. (8), and determine the range R_i in which it is located.

$$d_j' = |y_j' - y_{j+1}'| \tag{8}$$

3. Extract the secret qubits from d_j' by:

$$b_i = d'_j - l_i, \tag{9}$$

where the last $(2 + i)$ qubits of b_i are the target.
4. Reorganize all extracted qubits to get the original secret image and operator information.

So far, the accurate extraction of secret image without the original cover image is achieved. Simultaneously, we also extract operation information about the secret image. The extraction circuit is given in Fig. 10.

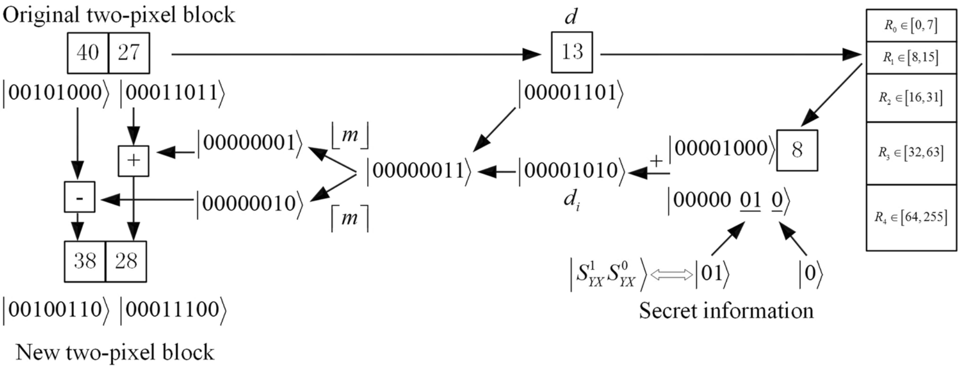


Figure 9. An illustration of the data embedding. The gray values of a sample two-pixel block are assumed to be (40, 27). The difference value is 13, which is in the range of 8 through 15. Therefore, the difference value is in the range of R_1, which means that three qubits are embedded in cover image, that is, the value of $|S^1_{YX} S^{01}_{YX}\rangle$ and operator information qubit is $|01\rangle$ and $|0\rangle$, respectively. It is added to the lower bound value 8 of R_2, resulting in a new difference value 10. Next, the new pixel values (38, 28) are obtained by the operational criterion in Eq. (7).

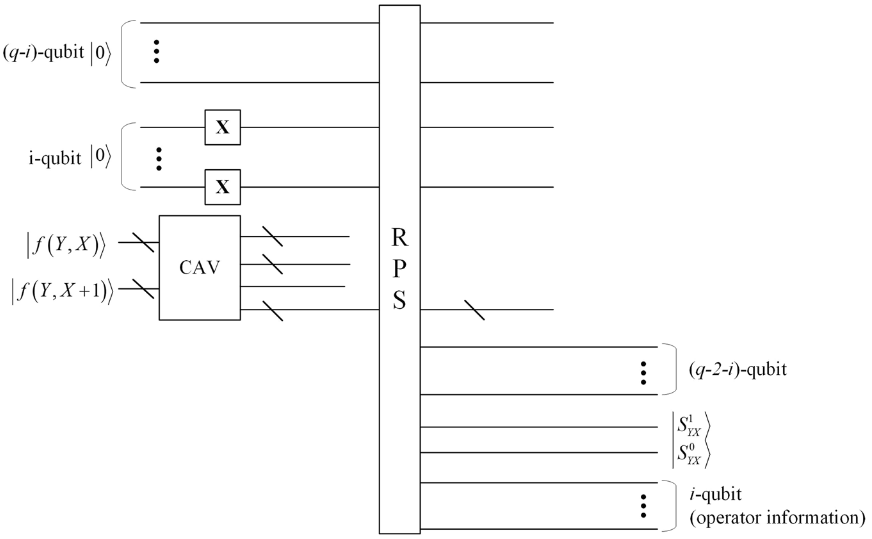


Figure 10. The extraction circuit. The last i + 2 qubits of output of RPS module which calculate the difference value of d_j' and the lower bound of the range are the target qubits, wherein last i qubits are the operator information and other two qubits are the value of secret image.

Time Complexity

In order to calculate the time complexity of quantum image processing algorithms, usually a basic gate is considered. For all complex unitary operations on many qubits can be expressed as compositions of all one-qubit quantum gates and the two-qubit quantum CNOT gate[38]. Therefore, the time complexity of any one-qubit gates and two-qubit gates is taken as a basic unit. The circuits of classification are dividing into one CAV module and (q-4) U_t modules. And in the embedding circuit shown in Fig. 8, there are including two CAV modules, five ADDER modules, four RPS modules, one QD module and one CS module.

For a q-qubits CAV module, it contains a CO module that includes q CNOT gates and q q-CNOT gates and a RPS module which complexity is $7q - 2$. Thus, the complexity of CAV module is:

$$q + q \times (12q - 11) + 7q - 2 = 12q^2 - 3q - 2 \tag{10}$$

And the q-qubit ADDER module is composed by 2q carry module (which circuit complexity is 3), q sum modules (which circuit complexity is 2) and an additional CNOT gate. So the circuit complexity of ADDER modules is:

$$2q \times 3 + q \times 2 + 1 = 8q + 1 \tag{11}$$

In addition, a q qubits QD module[37], the circuit complexity is $3q^3 + 6q^2 + q$. Reference[39] points out that a q-CNOT gate is equivalent to $(2q - 1)$ Toffoli gates and 1 CNOT gate with adequate ancillary qubits, and one Toffoli gate can be simulated by six CNOT gates. So the circuit complexity of CS module is:

Scheme	The time complexity
Reference[20]	$19n + 8$
Reference[25]	$3n + 2$
Reference[26] -first method	$18n^2 + 42n + 94$
Reference[26] -second method	$18n^2 + 90n + 504$
Reference[26] -third method	$18n^2 + 98n + 166$
Proposed scheme	$3q^3 + 53q^2 + 25q + 23$

Table 1. The comparison of complexity.

$$\sum\nolimits_{i=0}^{q-1}[6 \times (2i - 1) + 1] = 6q^2 - 11q \tag{12}$$

Thus, the complexity of embedding circuit is

$$\begin{aligned} &2 \times (12q^2 - 3q - 2) + 5 \times (8q + 1) + 4 \times (7q - 2) \\ &+(3q^3 + 6q^2 + q) + (6q^2 - 11q) \\ &= 3q^3 + 36q^2 + 52q - 7 \end{aligned} \tag{13}$$

For the Fig. 7, the complexity is:

$$\begin{aligned} &(12q^2 - 3q - 2) + \sum\nolimits_{i=3}^{q-1}[2(q - t) + 6(q - t)] \\ &= 16q^2 - 27q + 30 \end{aligned} \tag{14}$$

Thus, the total circuit complexity of data embedding is $3q^3 + 53q^2 + 25q + 23$, that is, $O(q^3)$.

For the extraction procedure, the circuit of classification is same as the embedding procedure which is given in Eq. (14) and the extraction circuit consists of one CAV module and one RPS module. Therefore, the circuit complexity is:

$$\begin{aligned} &(16q^2 - 27q + 30) + (12q^2 - 3q - 2 + 7q - 2) \\ &= 28q^2 - 23q + 26 \end{aligned} \tag{15}$$

that is $O(q^2)$.

We can see from the above, the complexity of embedding and extraction procedures is $O(q^3)$ and $O(q^2)$, respectively. This is only related to the qubits representing the gray scale. Compared with the complexity related to image size in the classical counterpart, our algorithm has a larger improvement than the classical algorithm.

Furthermore, we compare the time complexity of proposed scheme with other quantum information hiding schemes, in which the image size is $2^n \times 2^n$ and gray scale is 2^q. The results are enumerated in Table 1, we can see that the complexity of other schemes is related to the size of image, but the proposed scheme is related to the gray scale. Therefore, different from the complexity of other schemes that varies with image size, the complexity of the proposed scheme does not increase as the image gets larger.

Simulation Experiments and Discussion

In order to evaluate the proposed scheme comparing with the existing literature, in this section, simulations of the properties are demonstrated. All the simulations are based on a classical computer equipped with software Matlab R2014b. The cover images used in the simulation experiments are "Male", "Peppers" "Sailboat on lake" and "Airplane" with size of 256×256. Besides that, in order to facilitate the traceability, the operator information is a bit stream that full of quantum representation of the text "Quantum Text and Quantum Image"[30].

Invisibility.

The histogram analysis. Image histogram can be considered as a visualized tool for evaluating the visual effects caused by image steganography on cover images. The image histogram is a statistic of the gray level distribution in the image, that counting all the pixels in the image according to the gray value. Wherein, the abscissa is a gray level, and the ordinate is a frequency at which the gray level appears. By comparing the histogram graphs of two images one can judge whether the images similar or not. In image steganography algorithms, more similarity can be observed between the histogram of cover image and corresponding stego image, more invisibility can be obtained after the image steganography scheme manipulated.

Figure 11 indicates the histogram graphs of the six original images and the histogram graphs of their corresponding stego images where the image "Male" with size of 128×64 is considered as the secret image. According to the histogram graphs, it can be seen that the stego images are in good agreement with the original ones.

The peak signal-to-noise ratio (PSNR). Since the peak signal to noise ratio (PSNR) is generally used to evaluate the quality of the stego image, we adopt that to evaluate fidelity of our steganography scheme. The PSNR is defined as follows:

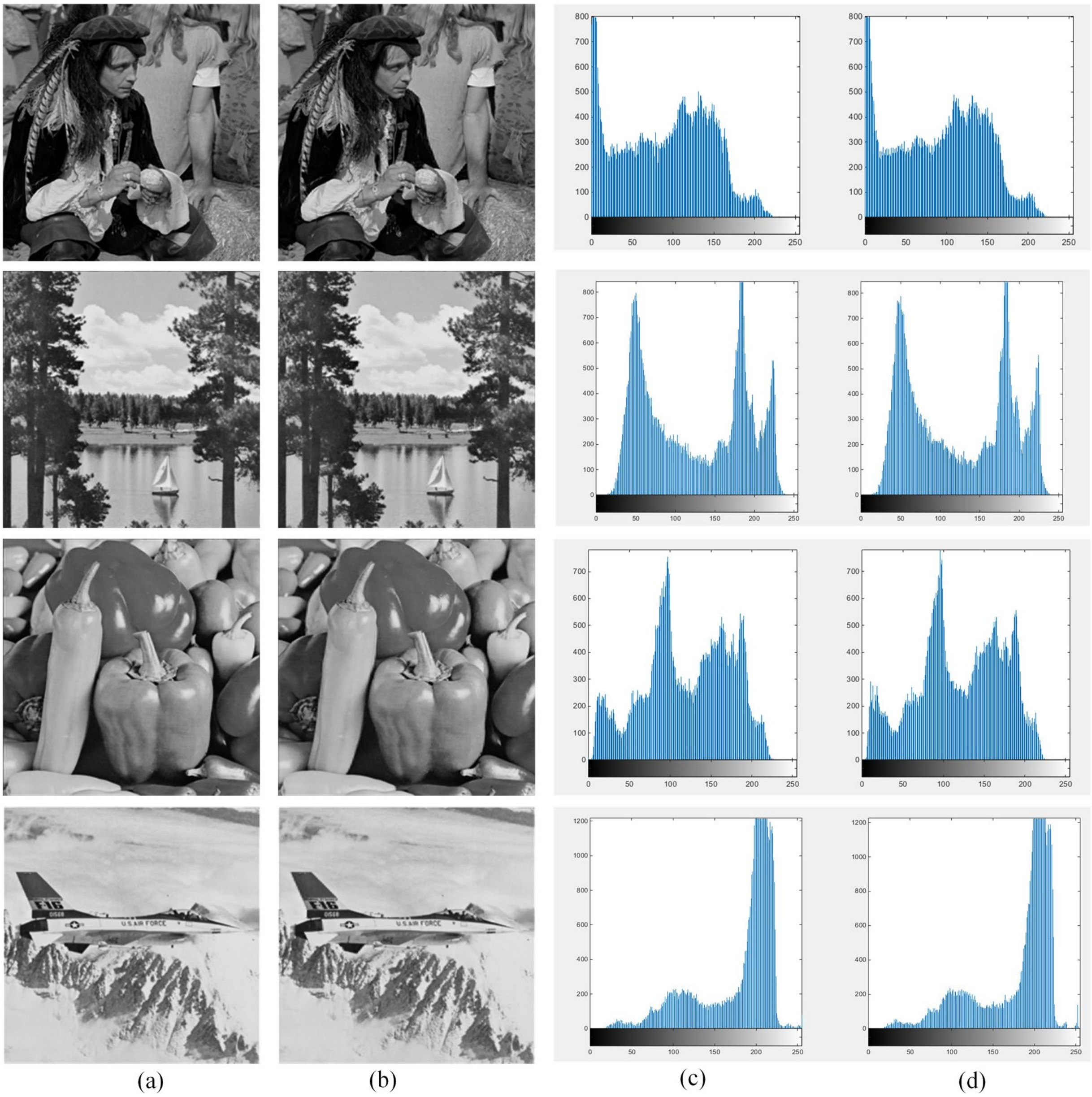


Figure 11. Each column from left to right is (**a**) original images (**b**) stego images (**c**) original image histogram graphs (**d**) stego image histogram graphs.

$$PSNR = 20\log_{10}\left(\frac{MAX_P}{\sqrt{MSE}}\right) \tag{16}$$

Herein, MAX_P is the maximum pixel value of the cover image, i.e., 255. MSE is defined as the mean squared error for two $m \times n$ images P and Q, where P and Q are associated with the stego image and the cover image, respectively.

$$MSE = \frac{1}{mn}\sum\nolimits_{i=0}^{m-1}\sum\nolimits_{j=0}^{n-1}[(P(i,\, j) - Q(i,\, j))^2] \tag{17}$$

The simulation results of PSNR are shown in Table 2, in which frequently-used images are selected as cover images, i.e., "Peppers", "Sailboat on lake" and "Airplane". Although the LSB based methods presented by Heidari *et al.*[27,29,30,40] has higher PSNR, our proposed algorithm also achieves a satisfactory visual quality from invisibility analyses.

Capacity. The capacity of quantum steganography scheme is defined as the ratio of the number of secret qubits and the number of cover pixels. Thus, the proposed scheme's capacity is given as follows:

Cover image	Secret image	PSNR
Peppers	Airplane	42.65
Sailboat on lake	Peppers	41.31
Airplane	Male	42.26

Table 2. The PSNR for the proposed scheme.

	Density		
Scheme	0.05	0.1	0.15
Reference[22]	15.03	12.15	10.20
Reference[25]	26.96	22.14	18.34
Reference[27]	—	31.30	30.14
Proposed scheme	41.90	38.92	37.39

Table 3. PSNR of extracted image under the salt and pepper noise.

$$\begin{aligned} C &= \frac{the\ num.\ of\ \sec retqubits}{thenum.\ of\ \cov erimagepixels} \\ &= \frac{q \times 2^{n-1} \times 2^{n-2} + m}{2^{2n}} = \frac{8 \times 2^{n-1} \times 2^{n-2} + m}{2^{2n}} = s(bit/pixel) \end{aligned} \tag{18}$$

where m and q are the embedded qubits of operator information and the gray scale of secret image, respectively. Therefore, the capacity of the proposed scheme is s that is greater than 1.

Robustness. *Robustness performance under noise.* Obviously, the secret image can be integrally extracted in a noise-free environment. However, the extraction procedure of the proposed scheme is not always carried out in a noiseless environment. The robustness of the proposed scheme under the salt and pepper noise is analyzed. Salt and pepper noises are applied with different density of from 0 to 0.15 into 256 × 256 stego image "Peppers". Peak signal-to-noise ratio (PSNR) is employed to evaluate the fidelity of the extracted secret image. The corresponding results from the stego images with noise are shown in Table 3. The table also shows the PSNR values of the scheme proposed in refs[22,25,27]. As can be seen from Table 3, the value of PSNR in our scheme is obviously higher than the other three schemes.

Robustness performance under attack. Since pure LSB based methods are easy detected, it is vulnerable to steganalysis. Regular and Singular (RS) steganalytic technique, first proposed in ref.[41], is very efficient in detecting the presence of a message in a gray image and to estimate its approximate size. The technique originated by analyzing the capacity for lossless data embedding in the LSB. Randomizing the LSB decreases the lossless capacity in the LSB plane, but it has a different influence on the capacity for embedding that is not constrained to one bit-plane. Thus, the lossless capacity turned out to be a very sensitive measure for the degree of randomization of the LSB plane. And the secret message length can be derived by inspecting the lossless capacity in the LSB plane.

In the proposed scheme, the differences of the gray values in the two-pixel blocks of the cover image are used as features to cluster the blocks into a number of categories of smoothness and contrast properties. Different amounts of data are embedded in different categories according to the degree of smoothness or contrast. Therefore, we have no significant change in the ratio of regular and singular groups compared to the original image. This means that RS technique cannot detect the embedded data in the cover image of the proposed scheme.

Conclusion

A new and traceable quantum steganography scheme for embedding secret image and operation information into cover image without producing noticeable changes has been proposed. The scheme is based on pixel value differencing which follows image edge effects and human visual system characteristics well. Pixels located in the edge area of the image are embedded with more secret information, including operator information for traceable secret images. Secret image and operation information are embedded into cover image by replacing the difference values of the two-pixel blocks of the cover image with similar ones in which qubits of embedded data are included. It is worth mentioning that the extraction process is absolutely blind. Furthermore, by embedding data in each adjacent pair of signals of images, the steganography scheme can also be easily extended to efficiently carry content-related messages such as captions or annotations in quantum audio and video.

Data availability

All data needed to evaluate the conclusions are available from the corresponding authors upon reasonable request.

Received: 13 February 2019; Accepted: 2 October 2019;
Published online: 22 October 2019

References

1. Vlasov, A. Y. Quantum Computations and Images Recognition. *arXiv:quant-ph/9703010* 4–10 (1996).
2. Beach, G., Lomont, C. & Cohen, C. Quantum Image Processing (QuIP). In *Applied Imagery Pattern Recognition Workshop* 2–7 (2003).
3. Kato, Z., Kato, T., Kondo, N. & Orii, T. Interstitial deletion of the short arm of chromosome 10: Report of a case and review of the literature. in. *Japanese Journal of Human Genetics* **41**, 333–338 (1996).
4. Venegas-Andraca, S. & Bose, S. Storing, Processing and Retrieving an Image using Quantum Mechanics. *Proc. SPIE - Int. Soc. Opt. Eng.* **5105**, (2003).
5. Venegas-Andraca, S. E. & Ball, J. L. Processing images in entangled quantum systems. *Quantum Inf. Process.* **9**, 1–11 (2010).
6. José, I. Latorre. Image compression and entanglement. Preprint at, https://arxiv.org/abs/quant-ph/0510031 (2005).
7. Le, P. Q., Dong, F. & Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Inf. Process.* **10**, 63–84 (2011).
8. Zhang, Y., Lu, K., Gao, Y. & Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **12**, 2833–2860 (2013).
9. Zhou, R., Tan, C. & Ian, H. Global and Local Translation Designs of Quantum Image Based on FRQI. *Int. J. Theor. Phys*. 1382–1398, https://doi.org/10.1007/s10773-017-3279-9 (2017).
10. Fan, P., Zhou, R., Jing, N. & Li, H. Geometric transformations of multidimensional color images based on NASS. *Inf. Sci. (Ny).* **340–341**, 191–208 (2016).
11. Zhou, R., Hu, W., Fan, P. & Ian, H. Quantum realization of the bilinear interpolation method for NEQR. *Sci. Rep.* **7**, 2511 (2017).
12. Jiang, N. & Wang, L. Quantum image scaling using nearest neighbor interpolation. *Quantum Inf. Process*. 1559–1571, https://doi.org/10.1007/s11128-014-0841-8 (2015).
13. Li, P. & Liu, X. Bilinear interpolation method for quantum images based on quantum Fourier transform. *Int. J. Quantum Inf.* **16**, (2018).
14. Sang, J., Wang, S. & Niu, X. Quantum realization of the nearest-neighbor interpolation method for FRQI and NEQR. *Quantum Inf. Process.* **15**, 37–64 (2016).
15. Zhou, R., Hu, W., Liu, X., Fan, P. & Luo, G. Quantum realization of the nearest neighbor value interpolation method for INEQR. *Quantum Inf. Process.* **17**, 166–203 (2018).
16. Zhang, Y., Lu, K., Xu, K., Gao, Y. & Wilson, R. Local feature point extraction for quantum images. *Quantum Inf. Process.* **14**, 1573–1588 (2015).
17. Yang, Y. G., Zhao, Q. Q. & Sun, S. J. Novel quantum gray-scale image matching. *Optik (Stuttg).* **126**, 3340–3343 (2015).
18. Jiang, N., Dang, Y. & Wang, J. Quantum image matching. *Quantum Inf. Process.* **15**, 3543–3572 (2016).
19. Zhou, R. G. *et al.* Similarity analysis between quantum images. *Quantum Inf. Process.* **17**, 1–12 (2018).
20. Song, X., Wang, S. & Abd, A. A. Dynamic watermarking scheme for quantum images based on Hadamard transform. *Multimed. Syst.* **20**, 379–388 (2014).
21. Johnson, N. F. & Jajodia, S. Exploring steganography: Seeing the unseen. *Computer (Long. Beach. Calif).* **31**, 26–34 (1998).
22. Jiang, N. & Wang, L. A Novel Strategy for Quantum Image Steganography Based on Moir ′ e Pattern. *Int. J. Theor. Phys*. 1021–1032, https://doi.org/10.1007/s10773-014-2294-3 (2015).
23. Jiang, N., Zhao, N. & Wang, L. LSB Based Quantum Image Steganography Algorithm. *Int. J. Theor. Phys.* **55**, 107–123 (2016).
24. Sang, J., Wang, S. & Li, Q. Least significant qubit algorithm for quantum images. *Quantum Inf. Process.* **15**, 4441–4460 (2016).
25. Miyake, S. & Nakamae, K. A quantum watermarking scheme using simple and small-scale quantum circuits. *Quantum Inf. Process.* **15**, 1849–1864 (2016).
26. Heidari, S. *et al.* Quantum red-green-blue image steganography. *Int. J. Quantum Inf.* **15**, 1750039 (2017).
27. Naseri, M. *et al.* A new secure quantum watermarking scheme. *Optik (Stuttg).* **139**, 77–86 (2017).
28. Heidari, S., Naseri, M., Gheibi, R. & Farouk, A. A New Quantum Watermarking Based on Quantum Wavelet Transforms. *Commun. Theor. Phys.* **67**, 732–742 (2017).
29. Heidari, S. & Farzadnia, E. A novel quantum LSB-based steganography method using the Gray code for colored quantum images. *Quantum Inf. Process.* **16**, 1–28 (2017).
30. Heidari, S., Gheibi, R., Houshmand, M. & Nagata, K. A Robust Blind Quantum Copyright Protection Method for Colored Images Based on Owner's Signature. *Int. J. Theor. Phys.* **56**, 2562–2578 (2017).
31. Hu, W., Zhou, R. & Fan, P. Quantum watermarking scheme through Arnold scrambling and LSB steganography. *Quantum Inf. Process.* **16**, 212–242 (2017).
32. Li, P., Zhao, Y., Xiao, H. & Cao, M. An improved quantum watermarking scheme using small-scale quantum circuits and color scrambling. *Quantum Inf. Process.* **16**, 127 (2017).
33. Zhou, R.-G., Hu, W., Fan, P. & Luo, G. Quantum color image watermarking based on Arnold transformation and LSB steganography. *Int. J. Quantum Inf.* **16**, 1–22 (2018).
34. Wu, D. C. & Tsai, W. H. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.* **24**, 1613–1626 (2003).
35. Le, P. Q., Iliyasu, A. M., Dong, F. & Hirota, K. Strategies for designing geometric transformations on quantum images. *Theor. Comput. Sci.* **412**, 1406–1418 (2011).
36. Vedral, V. & Ekert, A. Quantum Networks for Elementary Arithmetic Operations. *Phys. Rev. A* **54**, 147 (1996).
37. Khosropour, A., Aghababa, H. & Forouzandeh, B. Quantum Division Circuit Based on Restoring Division Algorithm. *2011 Eighth Int. Conf. Inf. Technol. New Gener*. 3–6, https://doi.org/10.1109/ITNG.2011.177 (2011).
38. Barenco, A. *et al.* Elementary gates for quantum computation. *Phys. Rev. A* **52**, 3457–3467 (1995).
39. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*. (Cambridge University Press, 2000).
40. Heidari, S. & Naseri, M. A Novel LSB Based Quantum Watermarking. *Int. J. Theor. Phys.* **55**, 4205–4218 (2016).
41. Fridrich, J., Goljan, M. & Du, R. Reliable Detection of LSB Steganography in Color and Grayscale Images. *Mm Sec Proc. Work. Multimed. Secur. New Challenges* 22–28 (2002).

Acknowledgements

This work is supported by the National Key R&D Plan under Grant No. 2018YFC1200200 and 2018YFC1200205; National Natural Science Foundation of China under Grant No. 61463016; and "Science and technology innovation action plan" of Shanghai in 2017 under Grant No. 17510740300. And Scientific Research Fund of Hunan Provincial Education Department (Grant No.18B420).

Author contributions

All authors contributed extensively to the work presented in this paper. R.Z. and G.L. conceived the study. J.L. designed the reversible logic circuits and analyzed the circuit complexity. G.L. and Y.L. performed the simulation-based experiment. Supervision and guidance were provided by R. Z. and G. L.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to R.-G.Z. or G.L.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.